RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: SBV2-T01

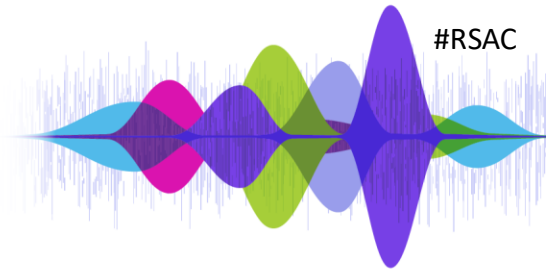
Intro to Physical Security

Terry Luan

Security Researcher
Physical Security Village
https://www.linkedin.com/in/terryluan12

Karen Ng

Security Researcher
GGR Security
https://www.linkedin/in/krn-ng



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

What is Bypass?

- When people think of physical hacking they often think of showier methods such as lockpicking
- However, there are plenty of other methods that can allow people to access locked-out locations known collectively as “Lock Bypass”

60

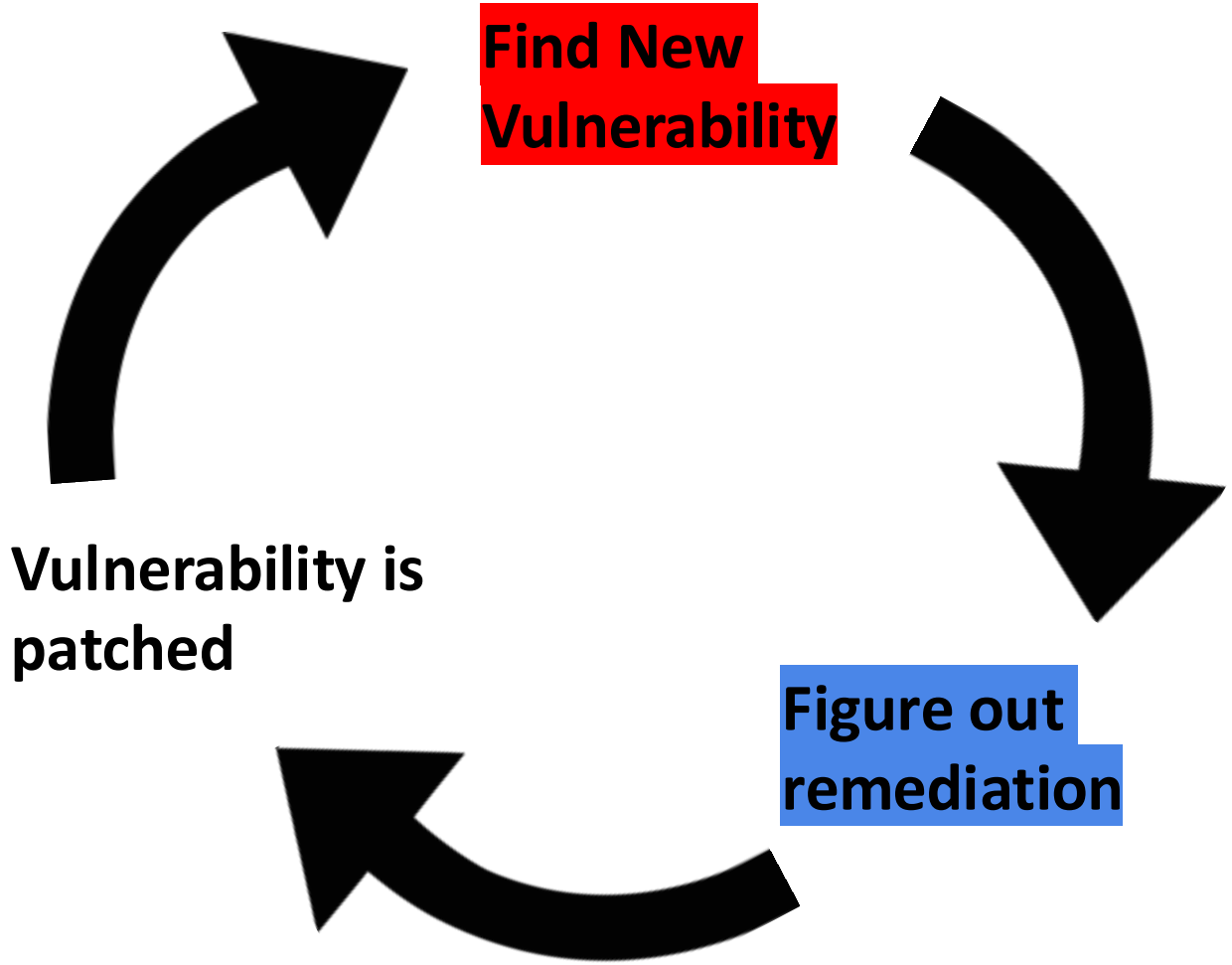
Why Bypass?

- Lock Bypass involves ignoring the lock altogether and finding alternative ways to open a door or avoid having to use a door altogether
- These methods are often much faster and more reliable than lockpicking, and is used more often in physical hacking
- It is an important part of a red-teamer's toolkit
- It doesn't matter how secure your servers are if someone can take one home and spend as much time as they need to crack it

Why Bypass?

- Finding physical security vulnerabilities and remediations for each bypass method is a constant back and forth between the red and blue team

A Constant Game of Cat and Mouse



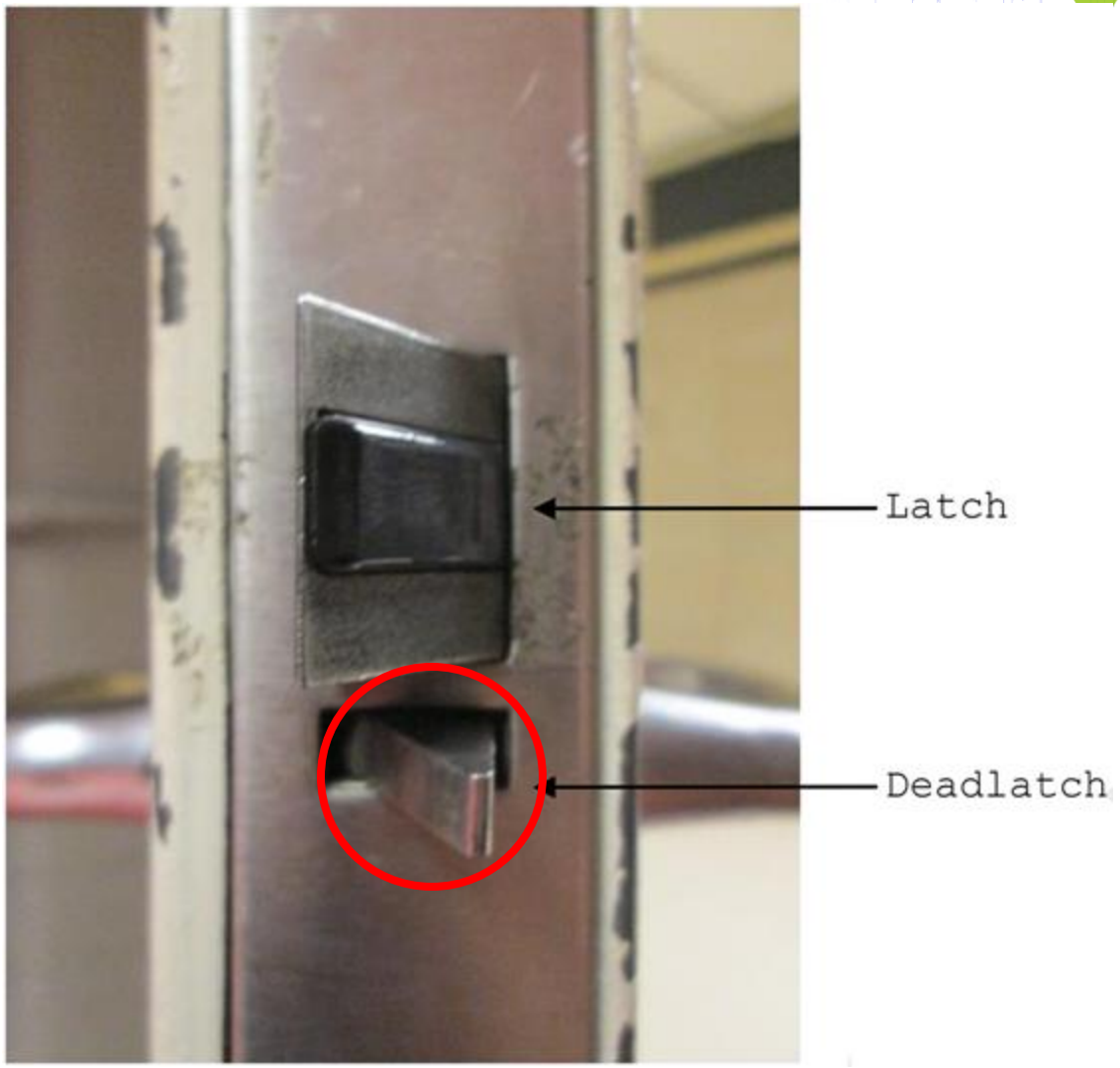
RSAC 2025 Conference

Door Latches

And Remediation of Latch-Based Bypasses

Many Voices.
One Community.

Door Latches & Deadlatches

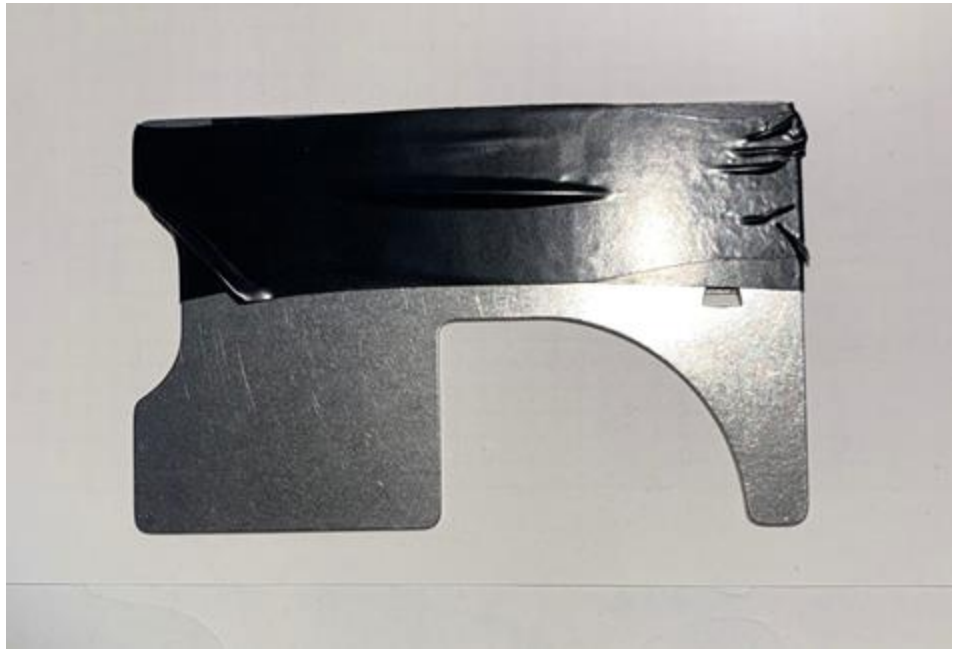


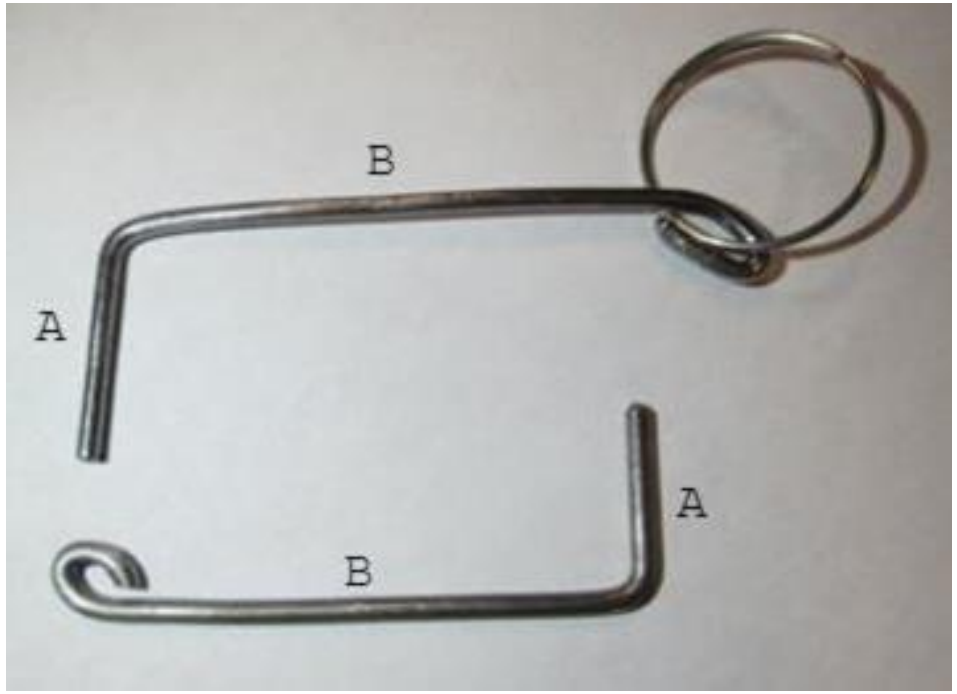
Deadlatches

De-actuating the Deadlatch

- Sometimes, the door is installed in such a way that the deadlatch is already inactivated
- Other times, the deadlatch is installed almost properly

The Tools

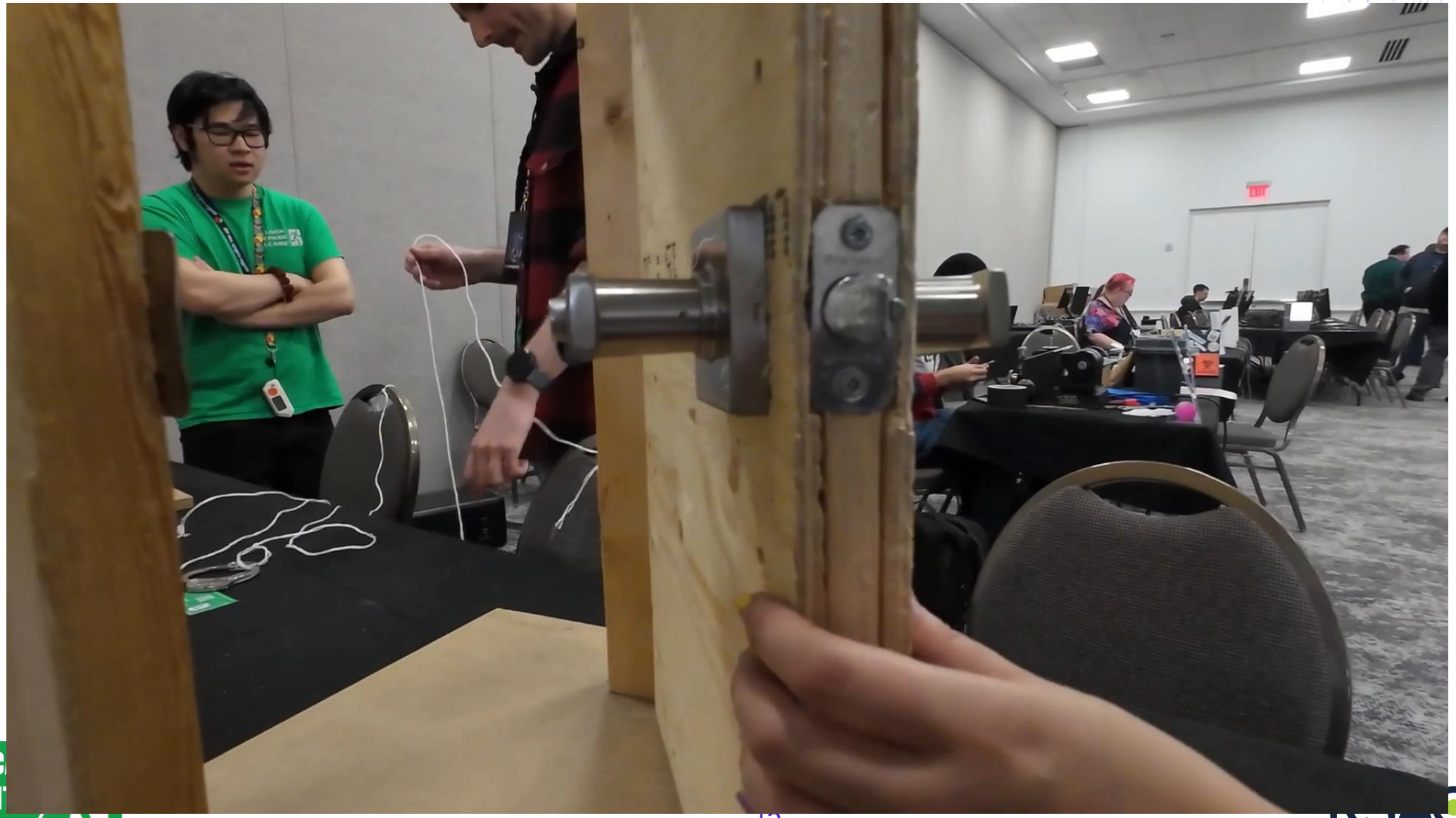




Instructions for Use (Pulling)

1. Place the latch slip tool behind the latch
2. Wiggle the latch slip to move the latch into the door
3. Without removing the tool from holding in the latch, pull the door open

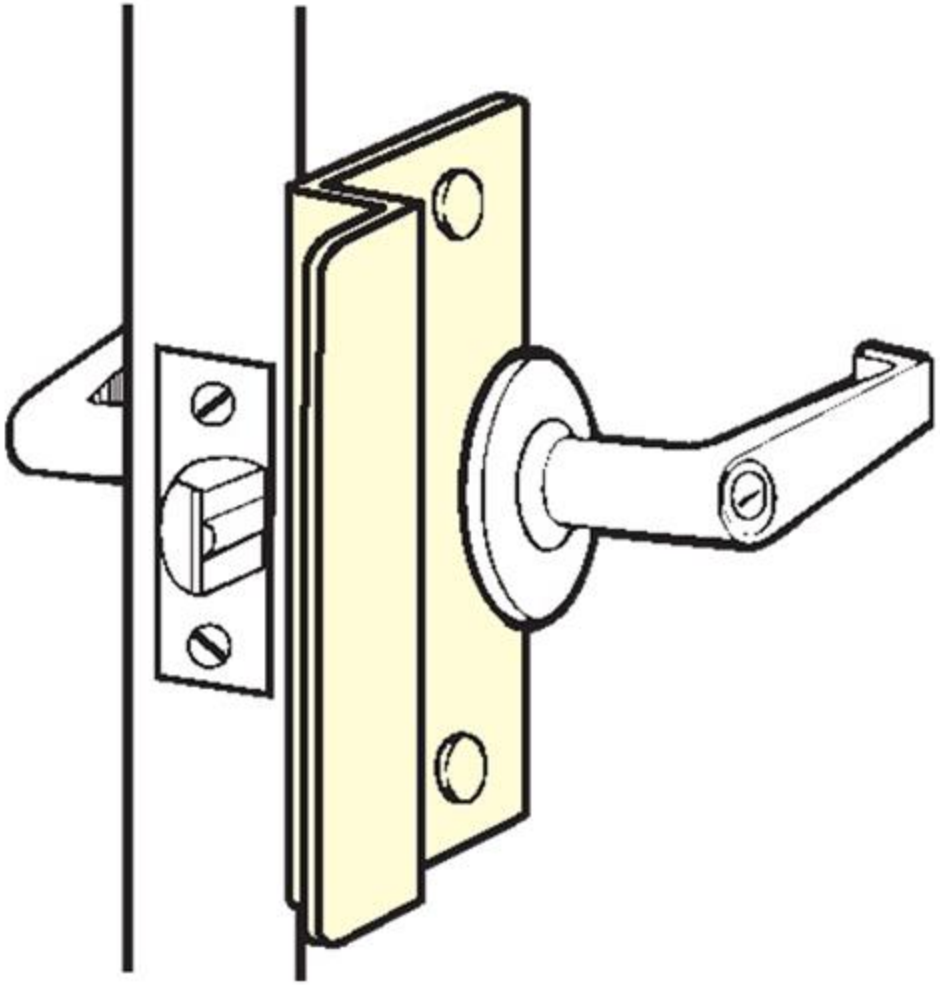
Instructions for Use



Remediation – The Deadlatch

- The easiest way to prevent latch slipping/pulling is to ensure that your doors are installed properly
  - the deadlatch is actuated when the door is closed
  - the strike plate is installed properly
  - the door fits the door frame properly

Remediation - Retrofit



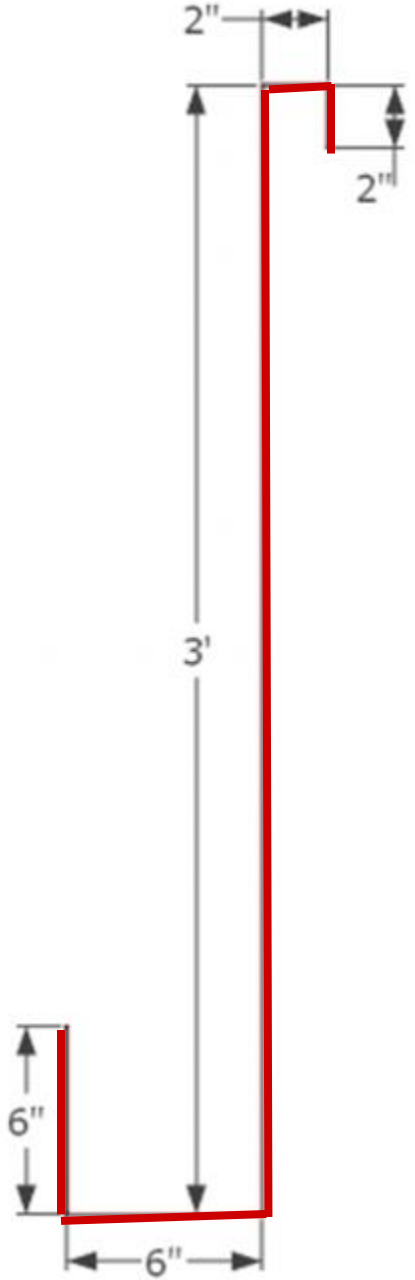
RSAC 2025 Conference

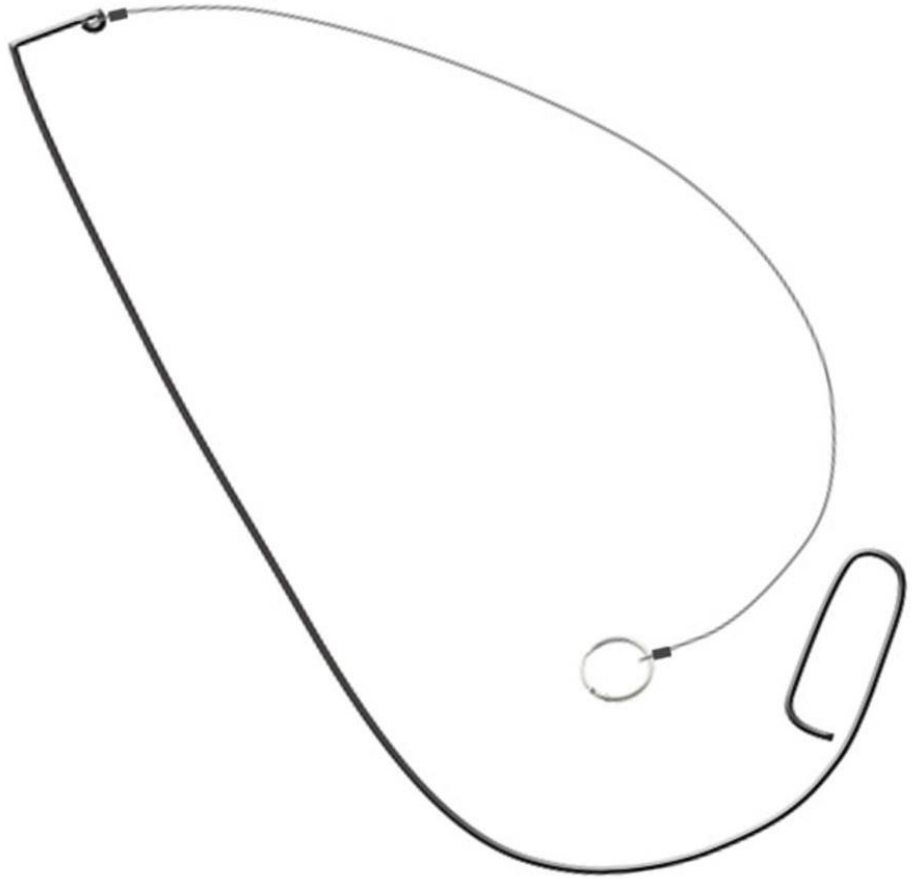
Door Handles

Wire-based Bypass (Part 1)

Many Voices.
One Community.

The Tool





Instructions for Use

1. Insert the tool under the door
2. Maneuver the tool until the top hook rests behind the door handle
3. Move the tool to the end of the handle
4. Pull on the string, actuating the lever

RSAC 2025 Conference

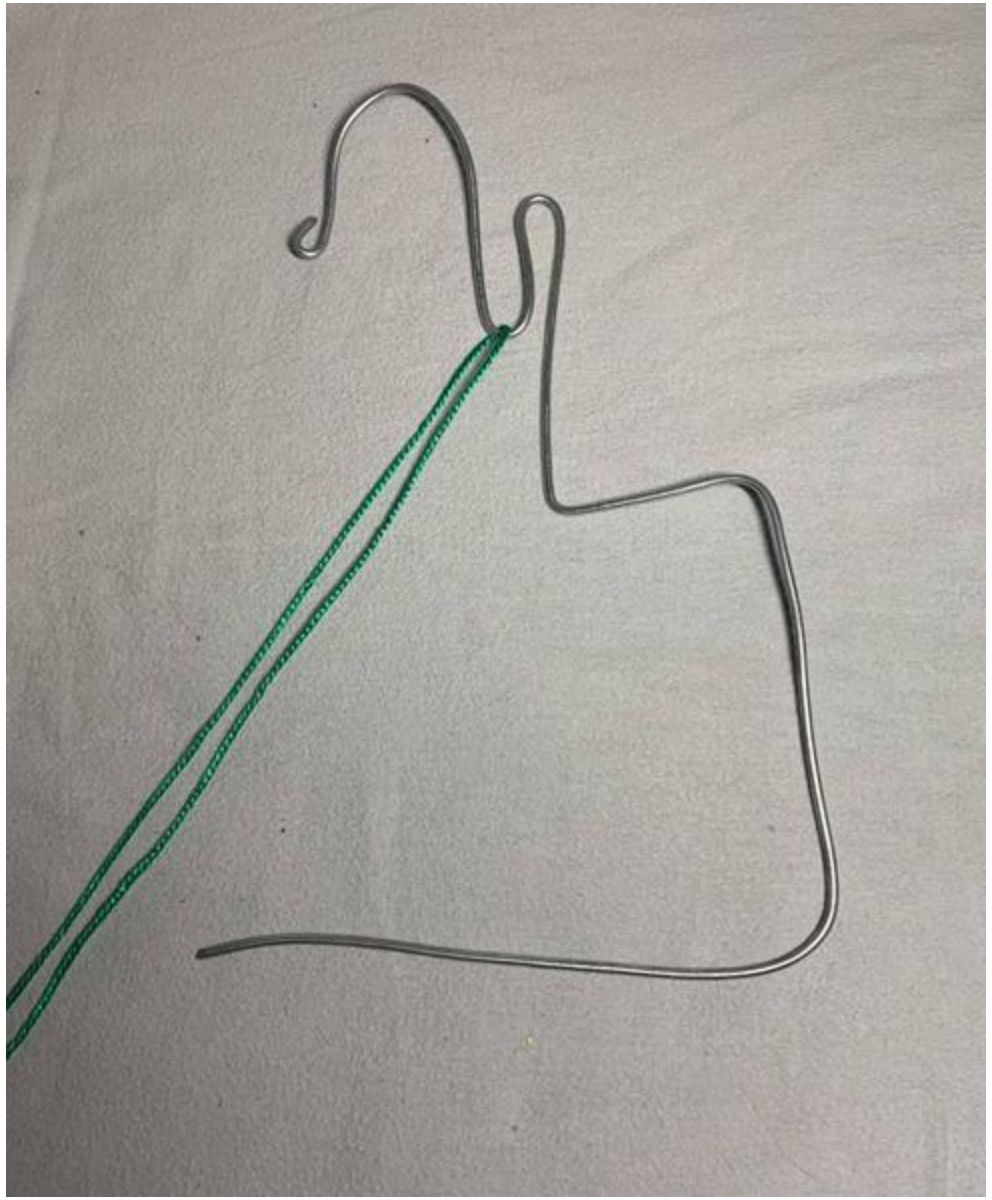
Crashbars

Wire-based Bypass

Many Voices.
One Community.

Crashbars

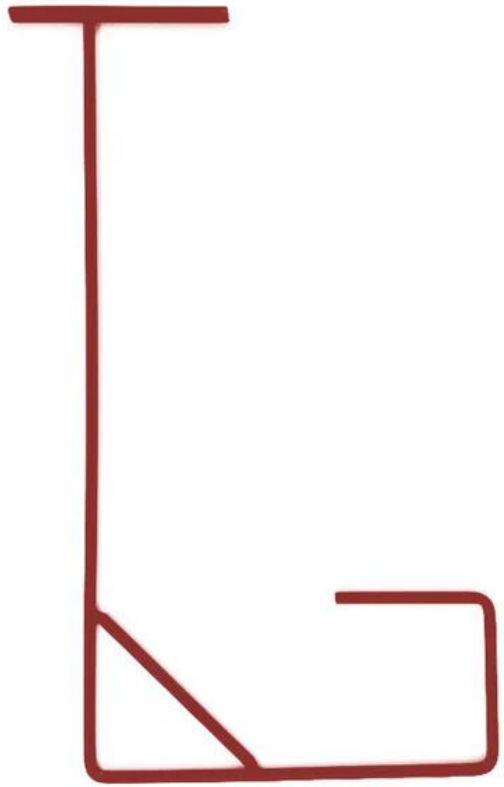
The Tool



Instructions for Use

1. Insert the tool through the side of the door (or start at the bottom and move up)
2. Rotate the tool until the hook lands on the crashbar
3. Pull down the string, pulling the crashbar towards the door and unlocking it from the inside

A Bonus Bypass



A Bonus Bypass

RSAC 2025 Conference

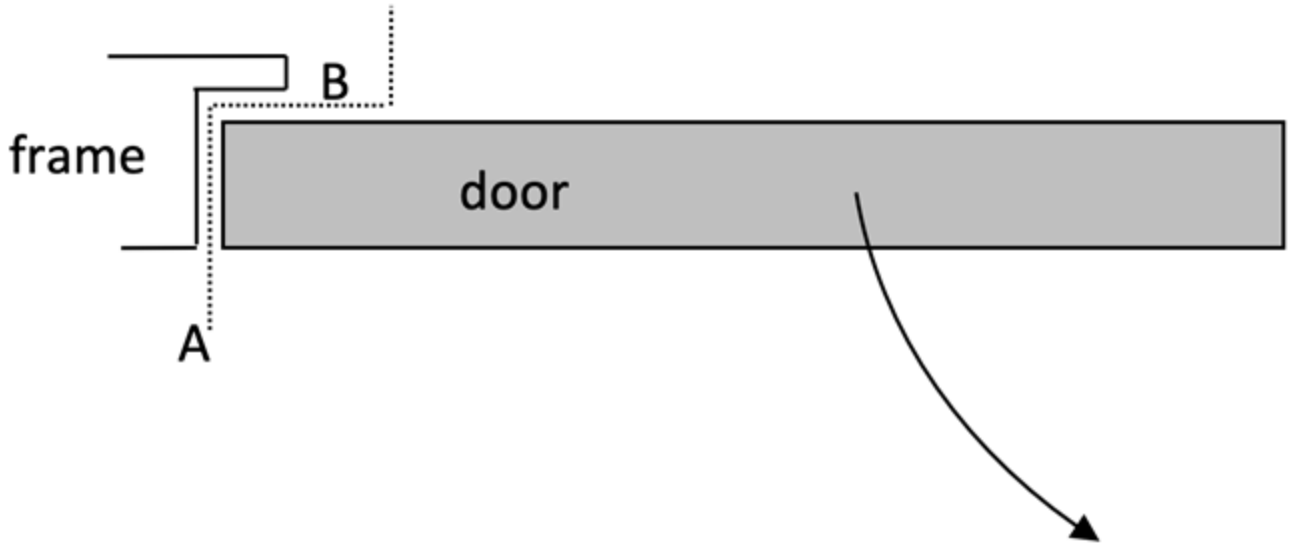
Remediation

Wire-based Bypass

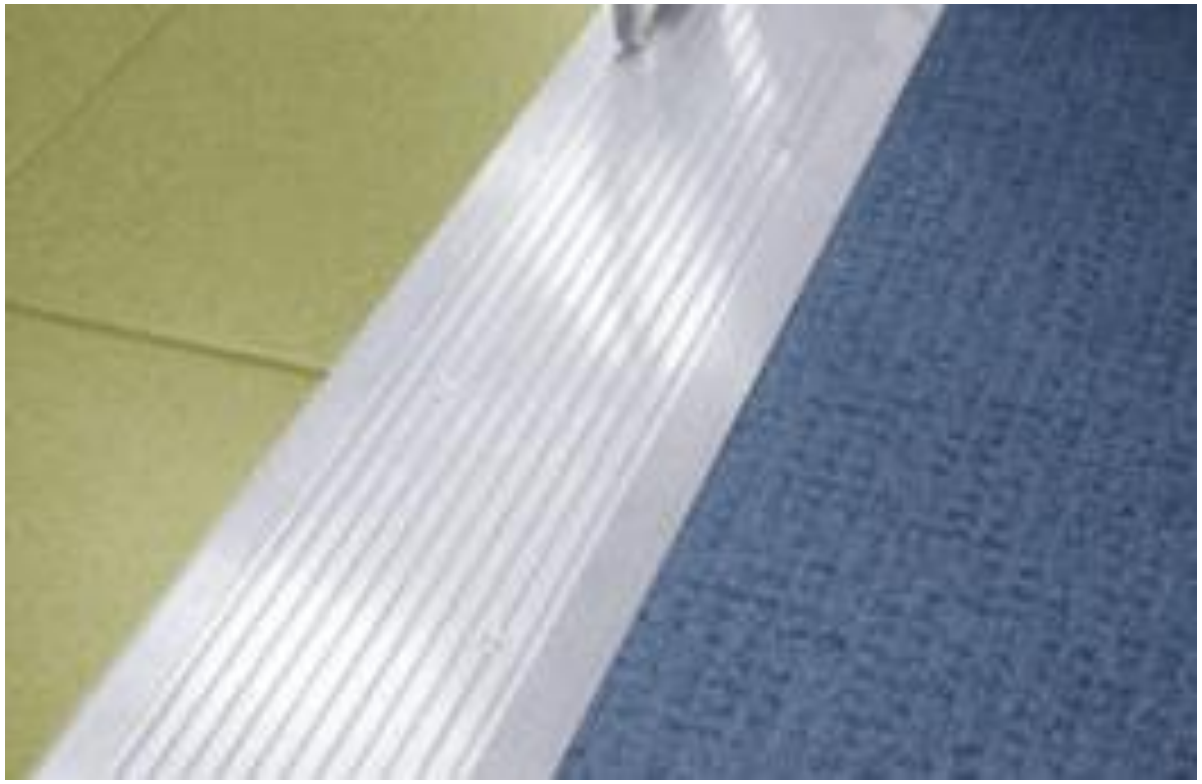
Many Voices.
One Community.

Remediation

- The easiest way to prevent this is to have a properly sized door for the frame, with little to no gap under and beside the door



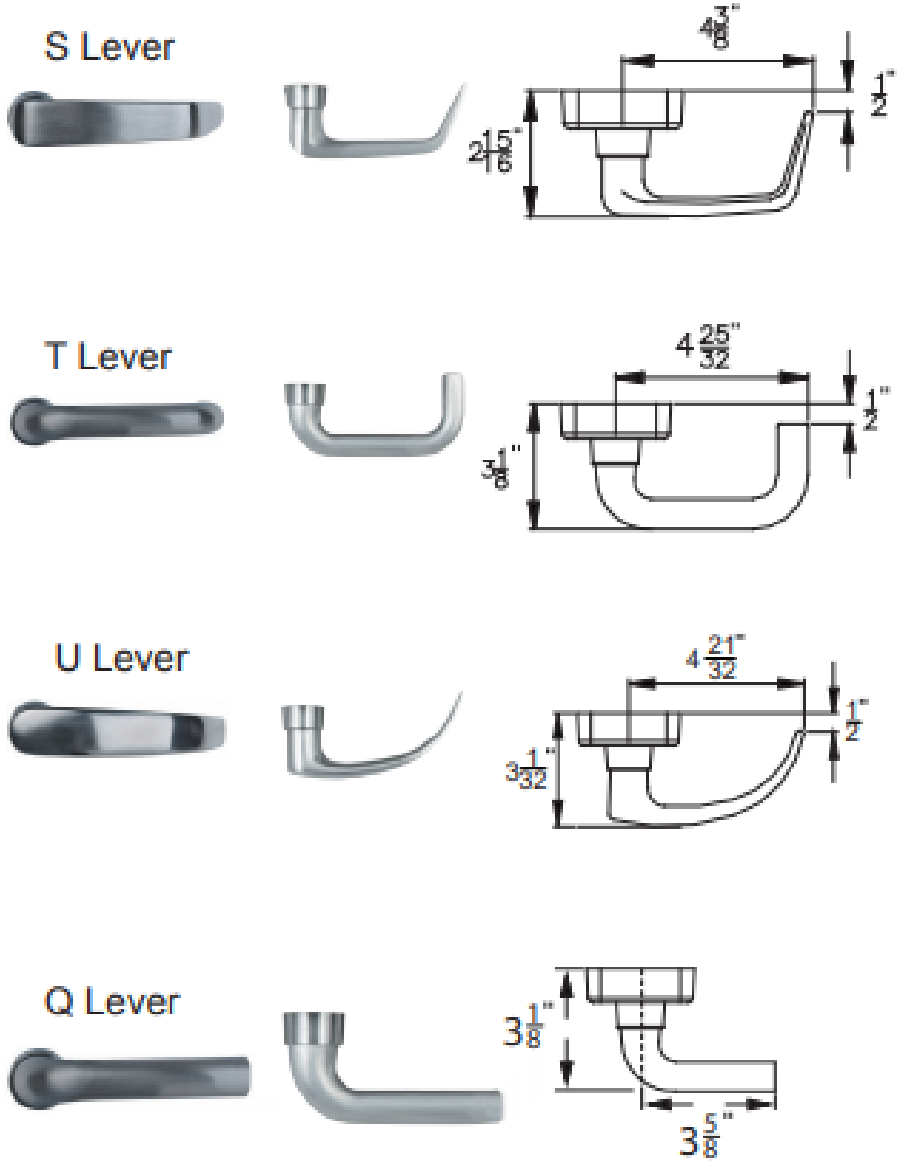
Remediation - Retrofit



Remediation - Retrofit

Remediation

- Certain lever-types are harder to use UDT's with



PHYSICAL SECURITY VILLAGE
RSAC 2025 Conference

Remediation - Retrofit

RSAC 2025 Conference

Deadbolts

Deadbolts

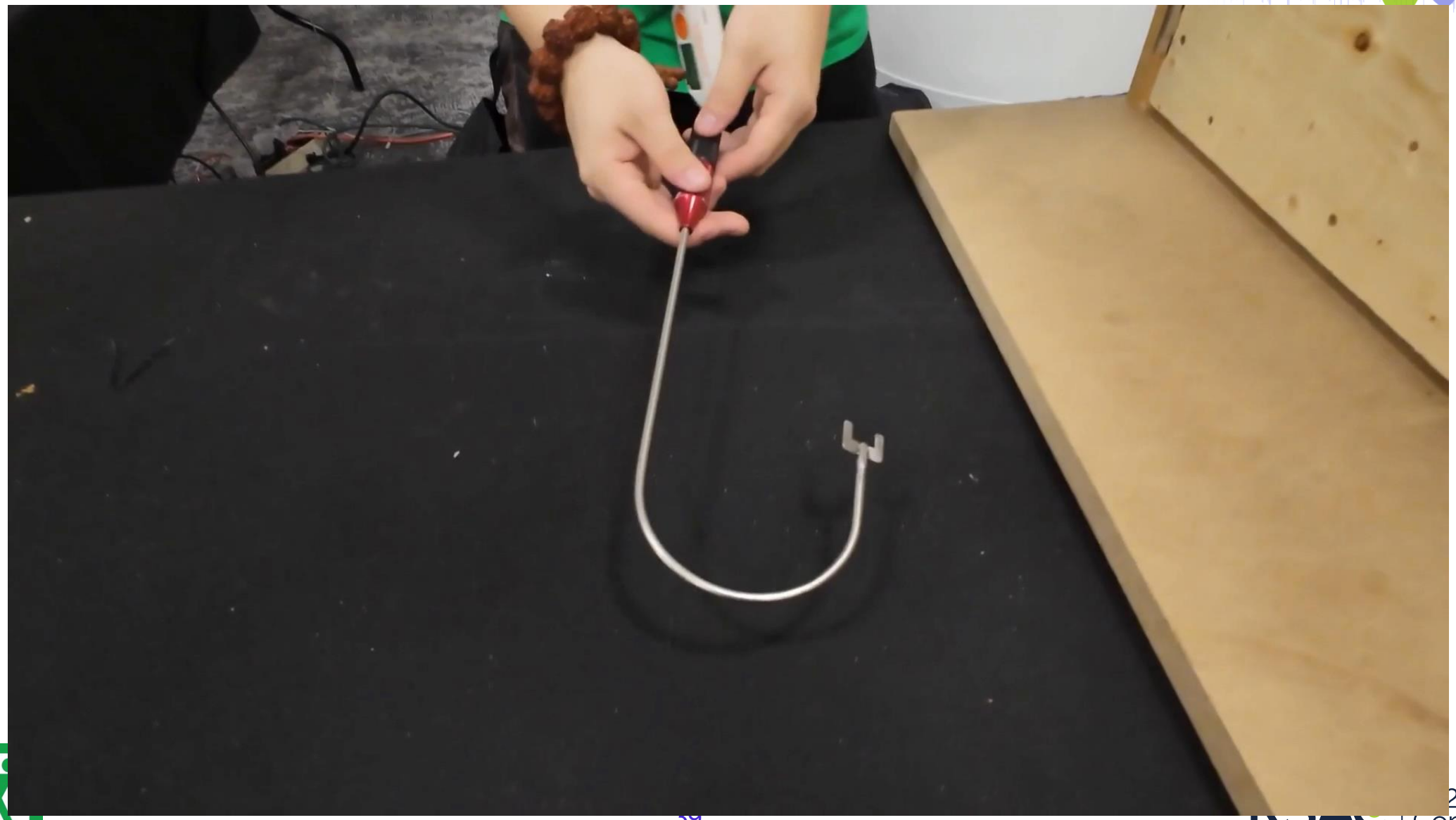
The Tool – J-Tool

Also sometimes called a thumb-turn bypass tool

Requirements

- Enough space between the frame to fit in the J-Tool
- Failing natural space, enough give in the door to fit in the J-Tool

Instructions for Use



Remediation

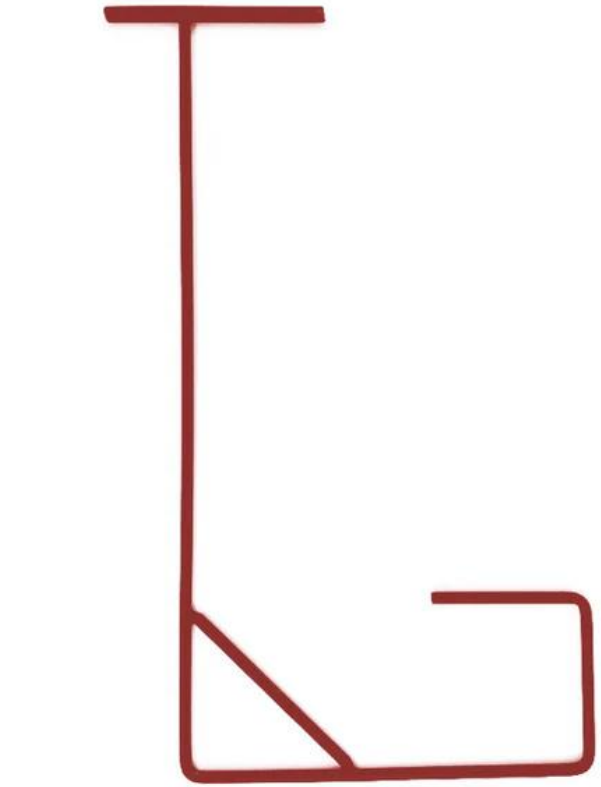
RSAC 2025 Conference

Pushbars

Pushbars

Method 1 – Double Door Tool (DDT)

- Confusingly, this tool is also sometimes called a J-Tool
- It also works on non-double doors



Requirements

- Enough space between the frame to fit in the double door tool OR enough give in the door to fit in the tool
- It is easier to do without a mullion (the middle bar that separates the two doors) but is still possible with one

COASTAL FIRE
TRAINING
EST. 2016

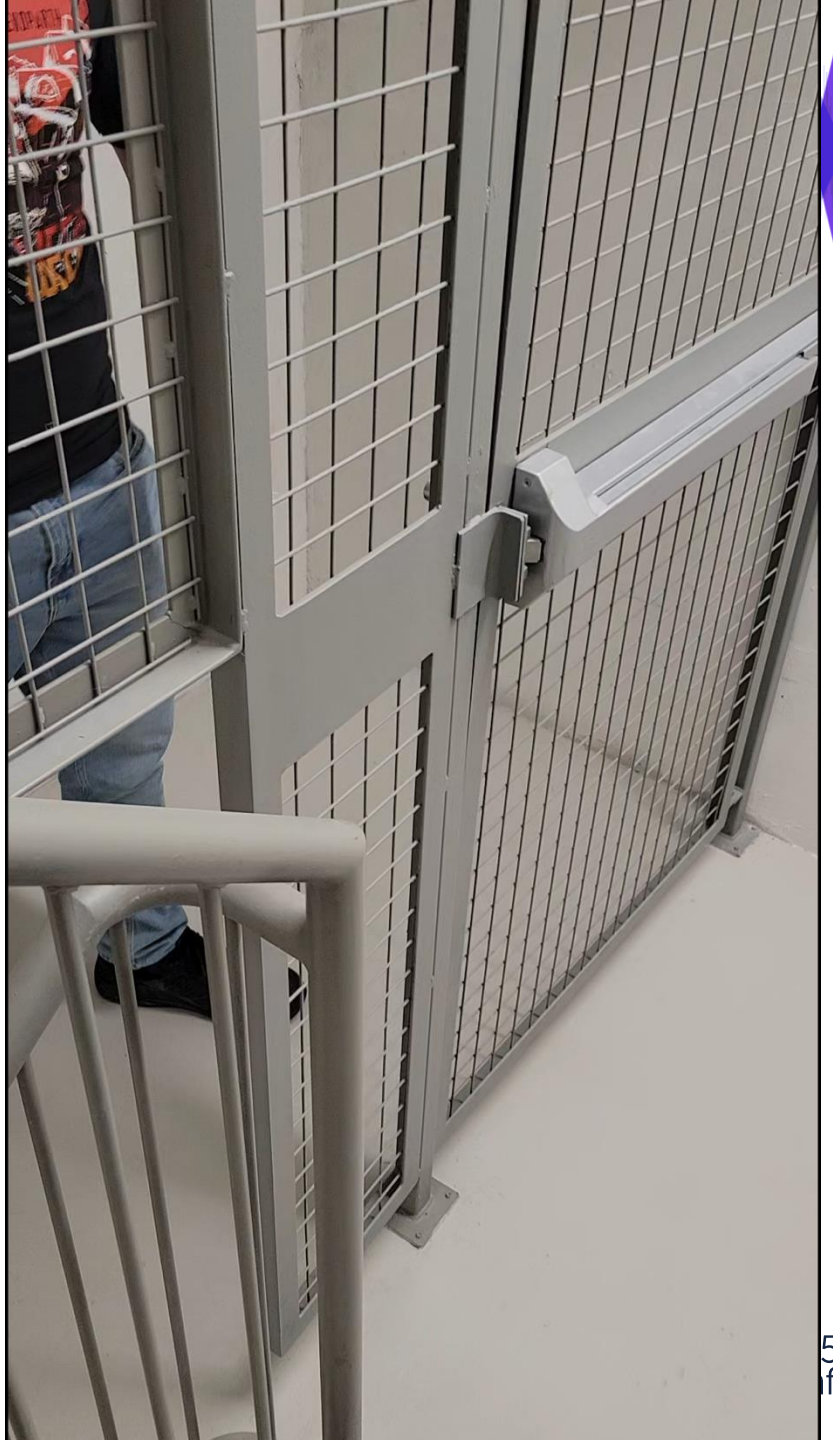
Method 2 – String

Requirements

- The pushbar must be either on a door with holes, or with room above and below the door

Instructions for Use

1. Feed the piece of string through the top of the door or through a hole above the pushbar
2. Move the string over the pushbar and through the bottom of the door or through a hole below the pushbar
3. Grab both ends of the string, and pull



RSAC 2025 Conference

Pulling Really Hard

You can do anything if you put your mind to it

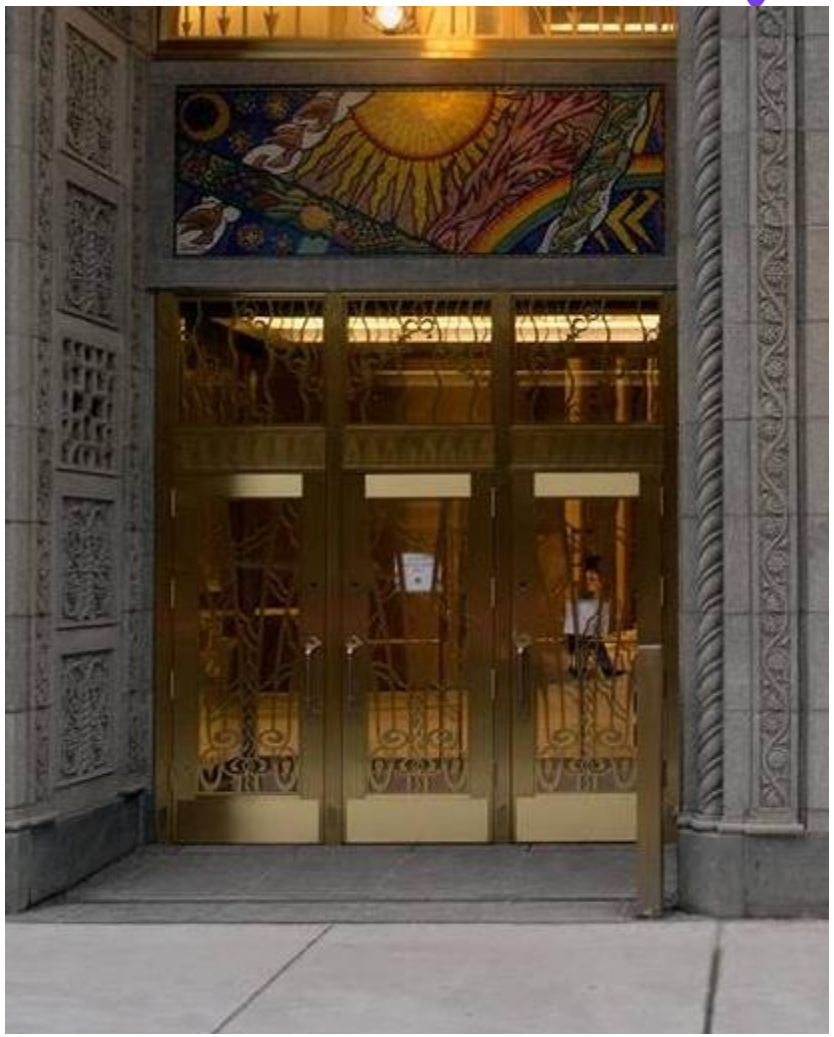
Many Voices.
One Community.

Pulling Really Hard

- “Pulling really hard” is a longstanding tradition of physical hackers.
- Many doors are loose in the frame and can be pulled open with a strong enough arm
- All you need for this bypass method is a strong pair of arms, and some elbow grease

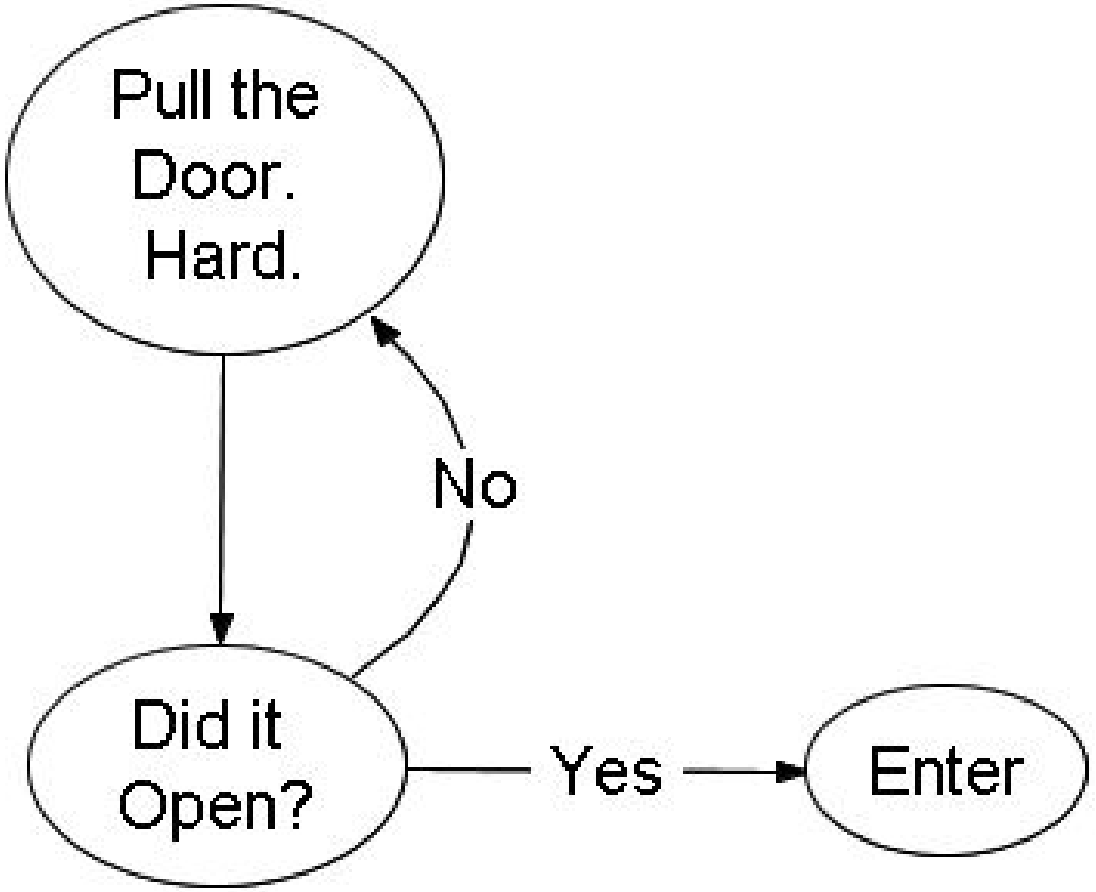
Requirements

- Not all doors are pullable, but a surprising number of them can be opened this way
- Look for “Springy, loose in the frame” that have some amount of flex
- Multibank doors are often pullable



INSTRUCTIONS FOR USE

Pull.



RSAC 2025 Conference

Removing Hinges

Method 1 - Removing The Hinges

The Tool

- A Screwdriver

Method 2 - Hinge Pin Removal

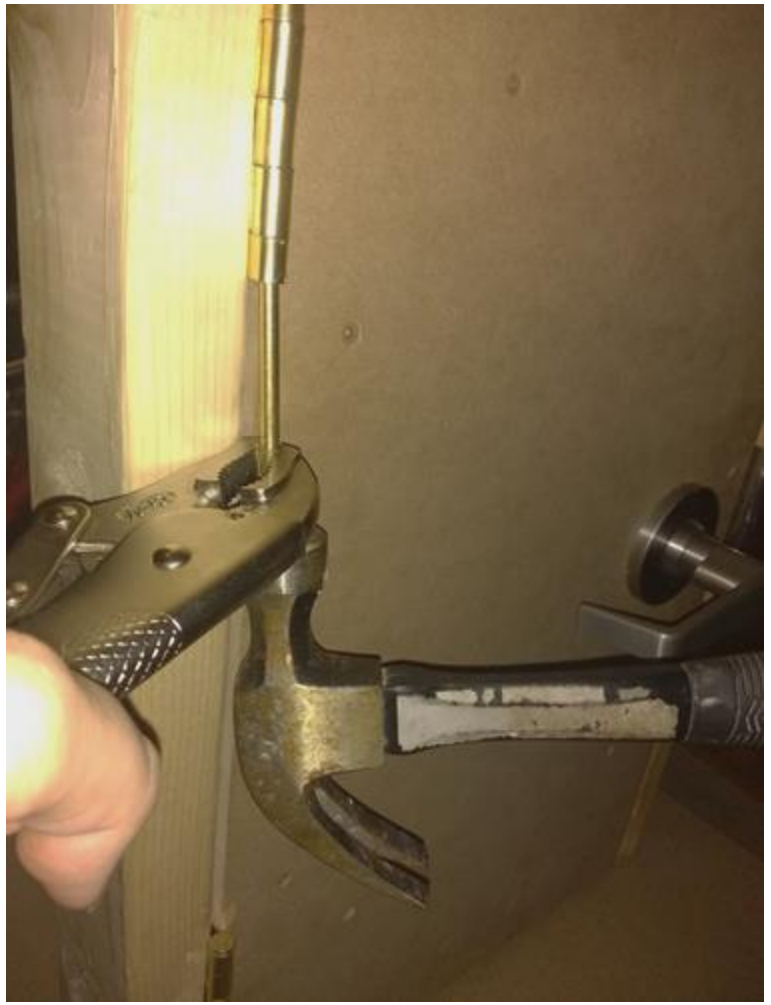
- Often, doors will have the pin of the hinge exposed
- The pin can be removed and allow the door to come off the frame

The Tool

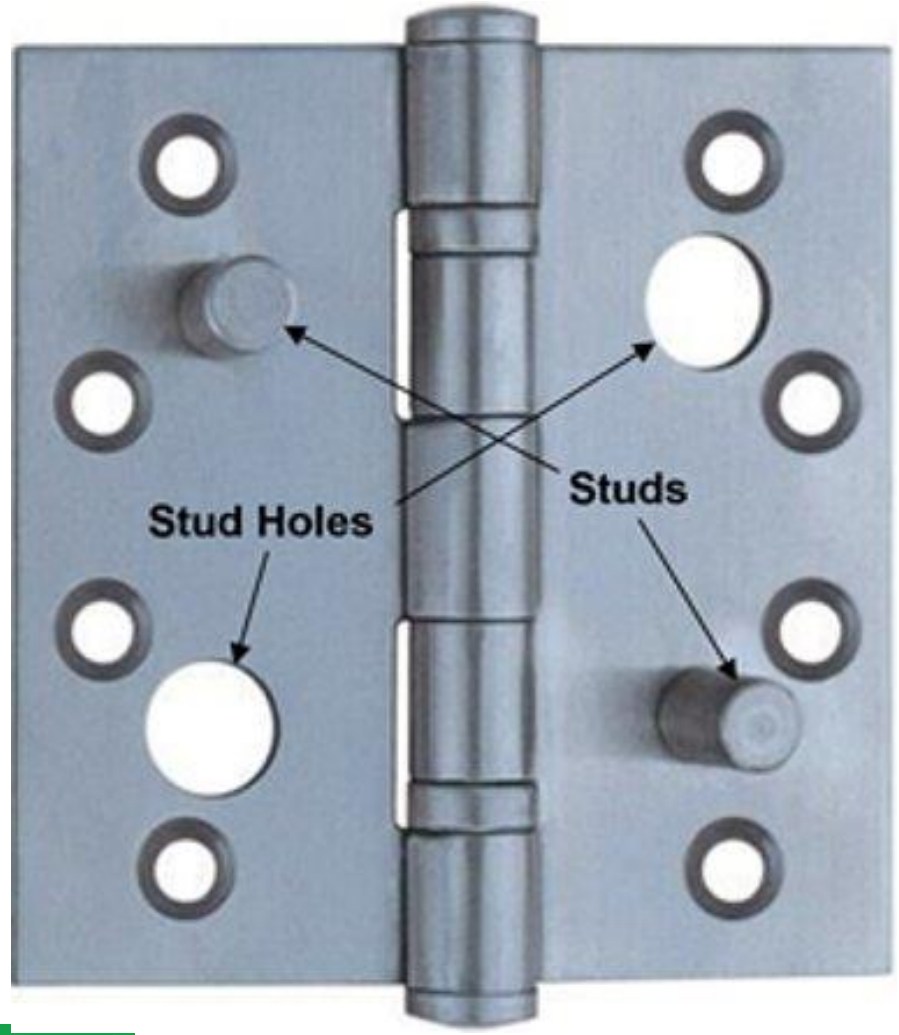
- A screwdriver (or nail)
- A hammer
- Vice Grips (optional)

Instructions for Use

1. Remove the bottom cap (if there is one)
2. Place the screwdriver under the hinge, with the point touching the bottom of the hinge pin
3. Gently tap on the screwdriver with the hammer until the pin can be pulled out
4. Repeat with the other hinge
5. Remove the door



Remediation - Retrofit



RSAC 2025 Conference

Button-Push Combination Locks

Button-Push Combination Locks

Master

Fob Cloning

Master Lock

+

LF_ANT_500UH
Portable ANT V3.0
Center Freq:125k
ELECHOUSE

=

Simplex

- The default code from the factory is (24)3
- Most people don't bother to set a new combination

CHANGE YOUR COMBINATIONS

Generally

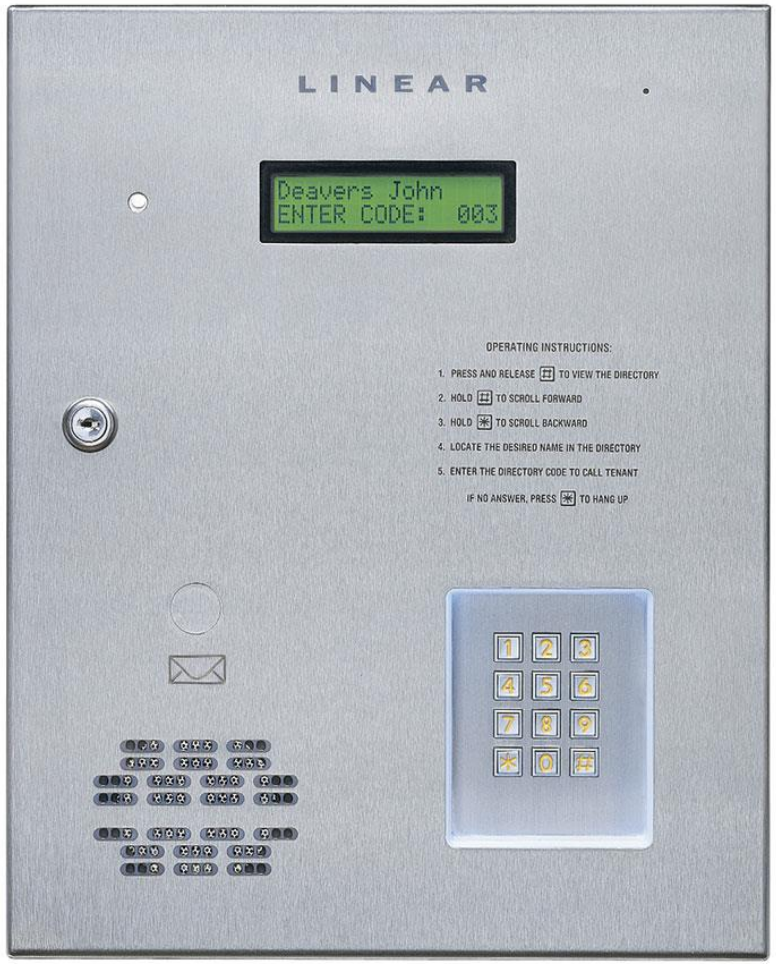
- If you suspect that someone unauthorized knows the combination to your button push combination lock…

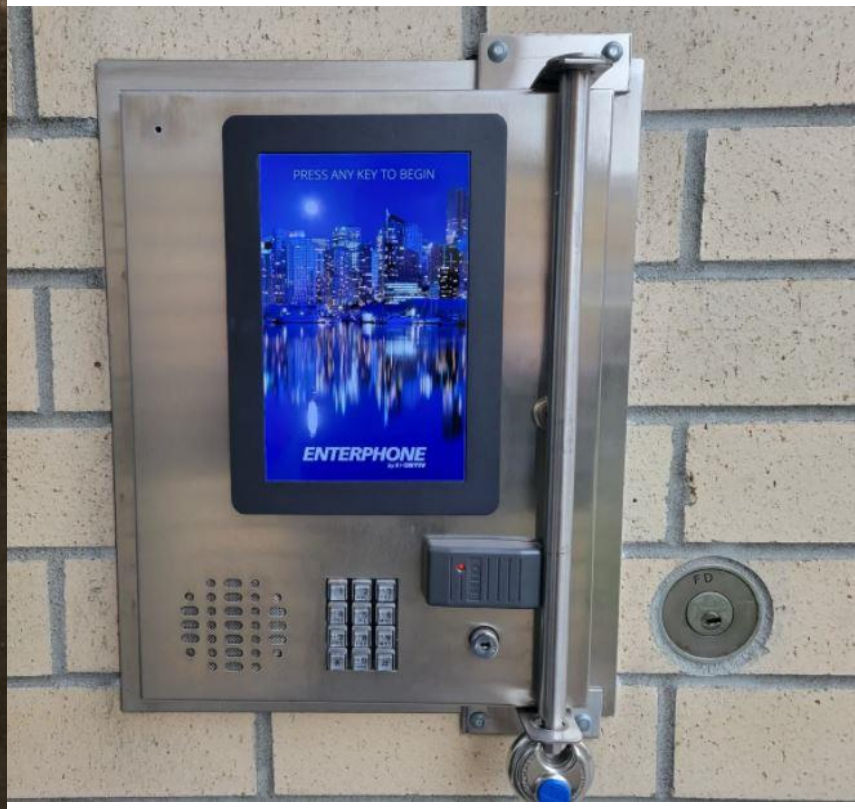
CHANGE YOUR COMBINATIONS

RSAC 2025 Conference

Enterphones

Enterphones


LINEAR
Deavers John
ENTER CODE: 003
OPERATING INSTRUCTIONS:
1. PRESS AND RELEASE # TO VIEW THE DIRECTORY
2. HOLD # TO SCROLL FORWARD
3. HOLD * TO SCROLL BACKWARD
4. LOCATE THE DESIRED NAME IN THE DIRECTORY
5. ENTER THE DIRECTORY CODE TO CALL TENANT
IF NO ANSWER, PRESS * TO HANG UP
1 2 3
4 5 6
7 8 9
* 0 #

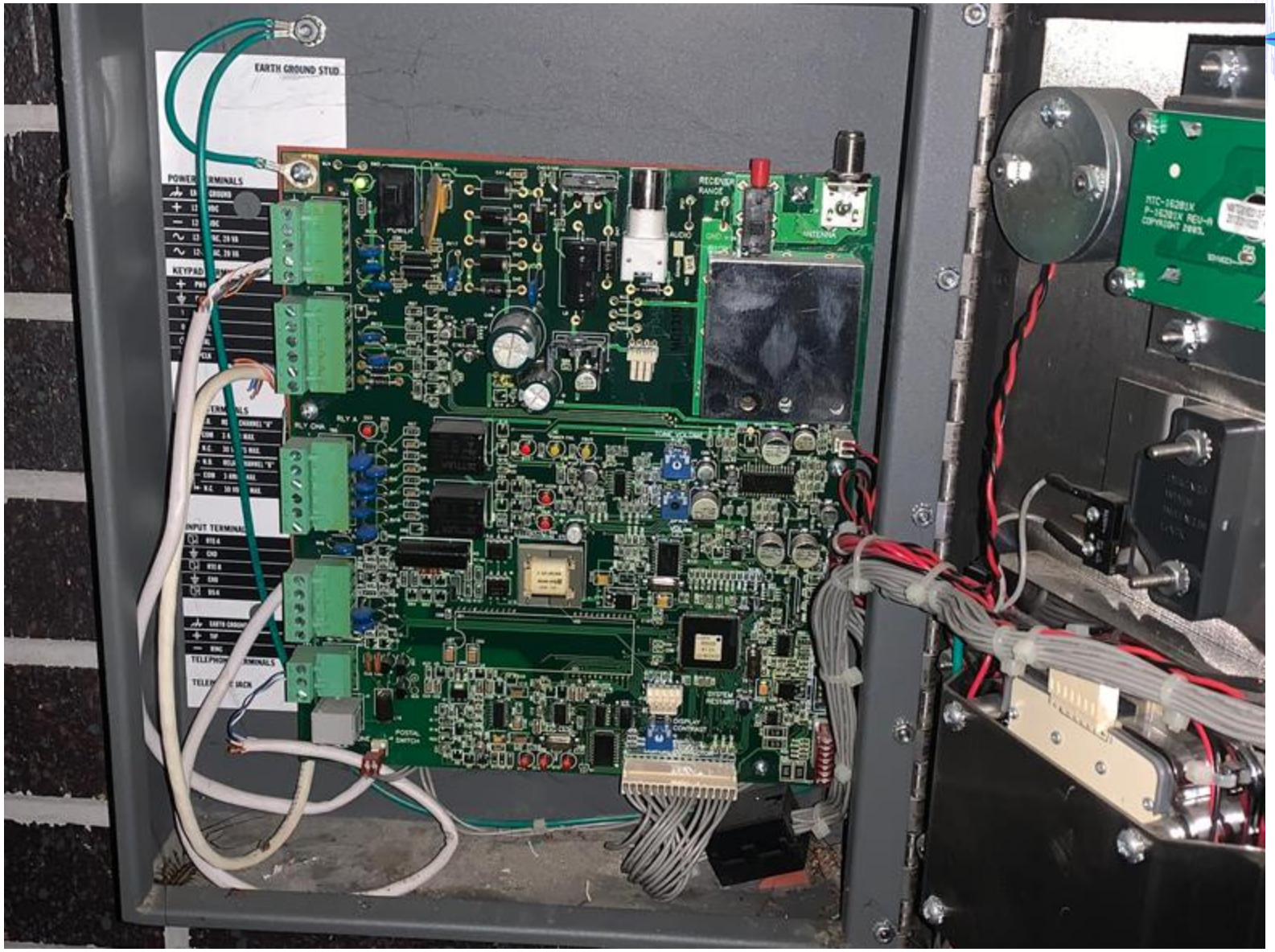


Enterphones

- The master code allows for you to configure the enterphone – from adding residents to adding entry codes
- [**CHANGE YOUR COMBINATIONS**
  b
- Again, people will often not bother to set a new combination

Enterphones

- There’s several major companies that make enterphones--Doorking, Door Guard, Linear, Mircom
- Enterphones are usually keyed-alike, meaning that one key can open enterphones made by the same company

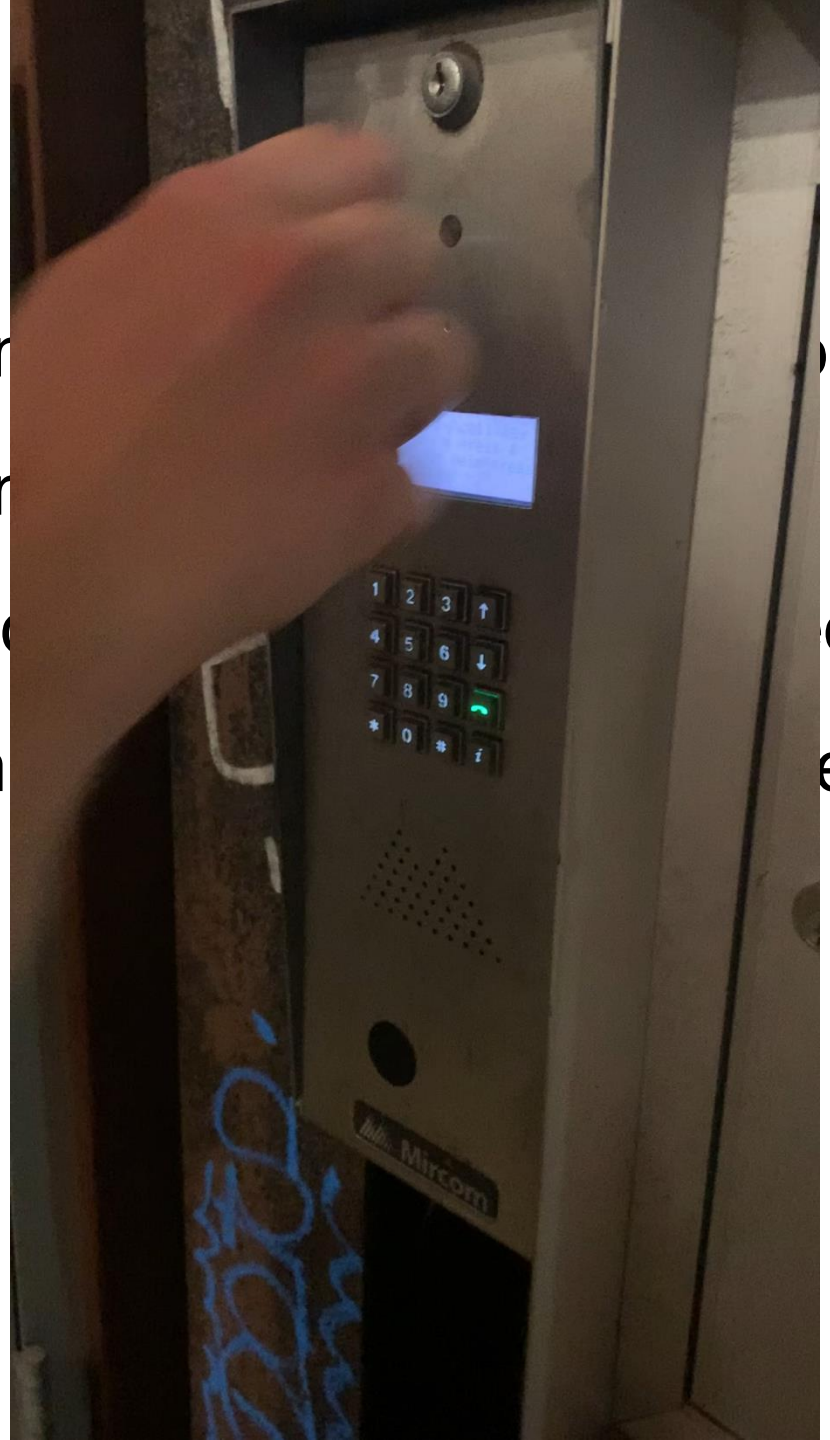

EARTH GROUND STUD
KEYPAD
INPUT TERMINALS
TELEPHONE TERMINALS

Instructions

1. Open the enterphone panel with the corresponding key
2. Find the unlocking mechanism
3. Use something conductive to jumper the mechanism
4. The door should unlock, as if someone buzzed you in

Instructions

1. Open the enterphor onding key
2. Find the unlocking r
3. Use something con chanism
4. The door should un ed you in



Remediation - Retrofits

CHANGE YOUR COMBINATIONS

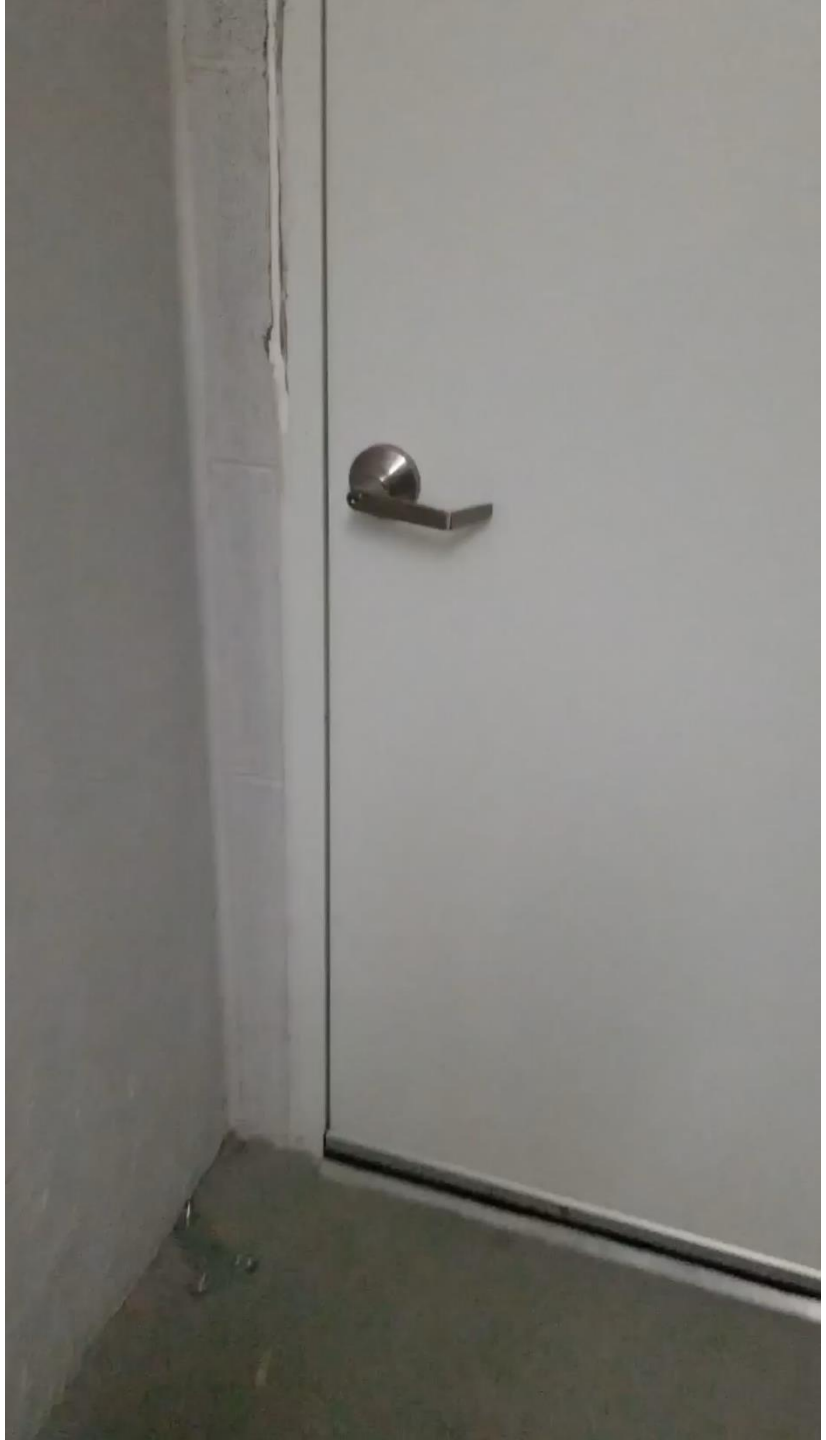
Remediation - Retrofits

- Enterphone covers and security bars can be used to prevent enterphones from being opened by key or by force

RSAC 2025 Conference

Wheelchair Buttons and Request to Exit Sensors

Wheelchair Buttons



PHYSICAL SECURITY VILLAGE

Request to Exit Sensors

- Some Request-to-Exit (REX) sensors are set up so they unlock and allow the person inside to leave the building, while preventing the door forced alarm from going off

Request to Exit Sensors

- Most REX sensors rely on passive infrared (PIR)
- If someone can trick the sensor into thinking there is someone on the inside, exiting the building, then it will allow them access

Maxxtro
SPRAYDUSTER
DRUCKGAS-REINIGER
BOMBE DÉPOUSSIÉRANTE
ARIA COMPRESSA
SPRAY DUSTER

Remediation

- Interlogix ~~makes~~ made a REX sensor that uses both PIR and radar to detect if someone was actually moving towards the door
- Dual technology REX sensors are still available from other manufacturers, but they're much less affordable

Remediation

- REX sensors are generally more convenient but less secure – for more secure areas, use a button or tap-in/tap-out system instead

RSAC 2025 Conference

Unlocked/Improperly Locked Doors

Many Voices.
One Community.

Unlocked/Improperly Locked Doors

Reasons a Door won't be locked

Human Error

- A worker propped it open and forgot to unprop it
- You came when the building was open and propped it
- Someone left clutter by the door that held it open
- The security guard or closing staff forgot to lock

Reasons a Door won't be locked

Environmental

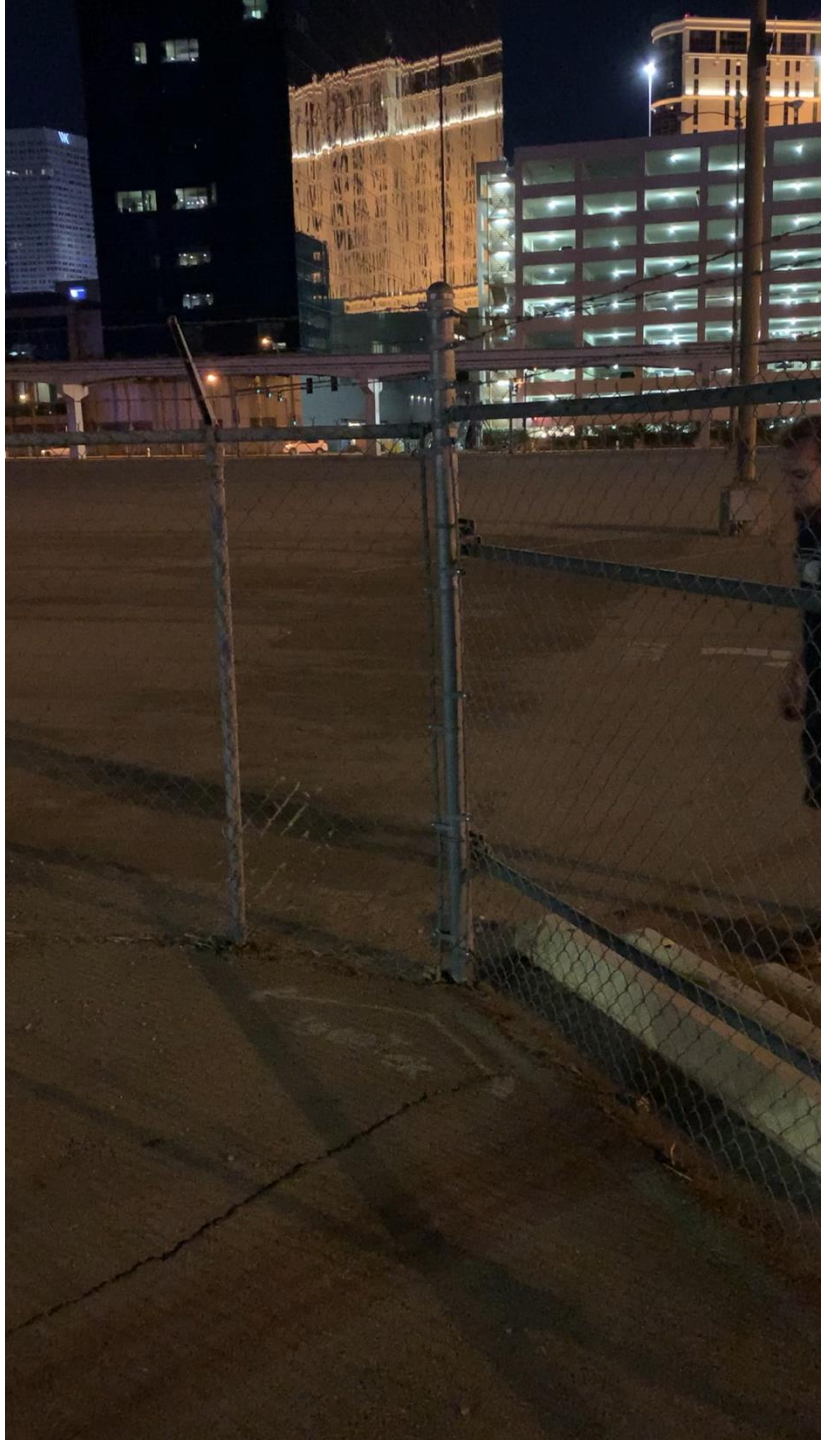
- Air pressure difference
- Warped door frame
- Poorly installed door or lock
- The door closer isn't working properly
- The lock is broken
- There is no lock there

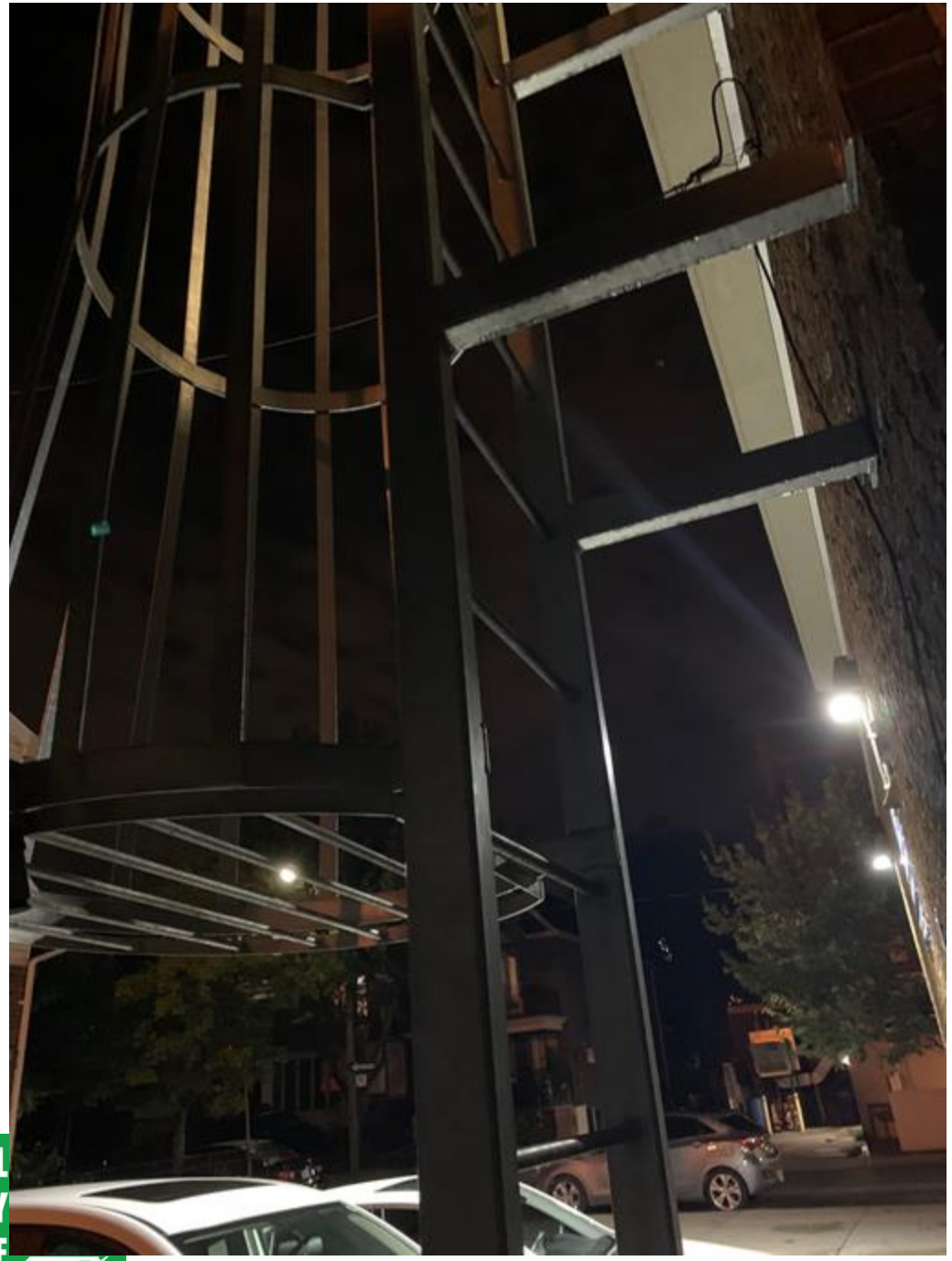
RSAC 2025 Conference

Ceilings, Windows, and Going Around

Going Under, Around, Above and Beyond

Many Voices.
One Community.





PHYSICAL SECURITY VILLAGE

erence

Other Important Security Implements

- Tailgating and other methods of social engineering needs to be prevented--promote a proper security culture within your workplace
- Alarms and sensors can be used in combination with remediations to prevent bypasses from being used without being caught
- Well-placed cameras can be used to detect, deter, and catch bad actors
- Without sensors, cameras, or other detection methods, anyone can get in with sufficient force!
- Response times matter! If a bad actor is detected, it is important to intercept them in the time between detection and them achieving their goal in your facility

Apply What You've Learned Today!

- Next week you should:
  - Identify potential points of vulnerabilities around your workplace
- In the first three months following this presentation you should:
  - Prioritize the potential vulnerabilities based on exploitability and level of risk
  - Develop possible solutions, including fixes and retrofits, to strengthen security
- Within six months you should:
  - Drive an implementation project to apply the appropriate retrofits, and fixes to remediate the most critical risks

PHYSICAL SECURITY VILLAGE

RSAC 2025 Conference

Many Voices.
One Community.

Thank you for listening!

For more information:

@physsec

or come find us at the Sandbox!